Configurazione Di SSL Anyconnect Con Autenticazione ISE E Attributo Class Per Il Mapping Criteri Di Gruppo

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[ASA](#)
[ISE](#)
[Risoluzione dei problemi](#)
[Scenario di lavoro](#)
[Scenario non lavorativo 1](#)
[Scenario non lavorativo 2](#)
[Scenario non lavorativo 3](#)
[Video](#)

Introduzione

In questo documento viene descritto come configurare Secure Sockets Layer (SSL) Anyconnect con Cisco Identity Services Engine (ISE) per il mapping degli utenti a Criteri di gruppo specifici.

Contributo di Amanda Nava, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AnyConnect Secure Mobility Client versione 4.7
- Cisco ISE 2.4
- Cisco ASA versione 9.8 o successive.

Componenti usati

Il contenuto di questo documento si basa su queste versioni software e hardware.

- Adaptive Security Appliance (ASA) 5506 con software versione 9.8.1
- AnyConnect Secure Mobility Client 4.2.00096 su Microsoft Windows 10 a 64 bit.

- ISE versione 2.4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Nell'esempio, gli utenti di Anyconnect si connettono direttamente senza poter selezionare il gruppo di tunnel dal menu a discesa, in quanto vengono assegnati da Cisco ISE a specifici Criteri di gruppo in base ai loro attributi.

ASA

Server AAA

```
aaa-server ISE_AAA protocol radius
aaa-server ISE_AAA (Outside) host 10.31.124.82
key cisco123
```

AnyConnect

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
anyconnect enable

tunnel-group DefaultWEBVPNGroup general-attributes
address-pool Remote_users
authentication-server-group ISE_AAA

group-policy DfltGrpPolicy attributes
banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
vpn-simultaneous-logins 0
vpn-tunnel-protocol ssl-client

group-policy RADIUS-USERS internal
group-policy RADIUS-USERS attributes
banner value YOU ARE CONNECTED TO ### RADIUS USER AUTHENTICATION###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list value SPLIT_ACL

group-policy RADIUS-ADMIN internal
group-policy RADIUS-ADMIN attributes
banner value YOU ARE CONNECTED TO ###RADIUS ADMIN AUTHENTICATION ###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list none
```

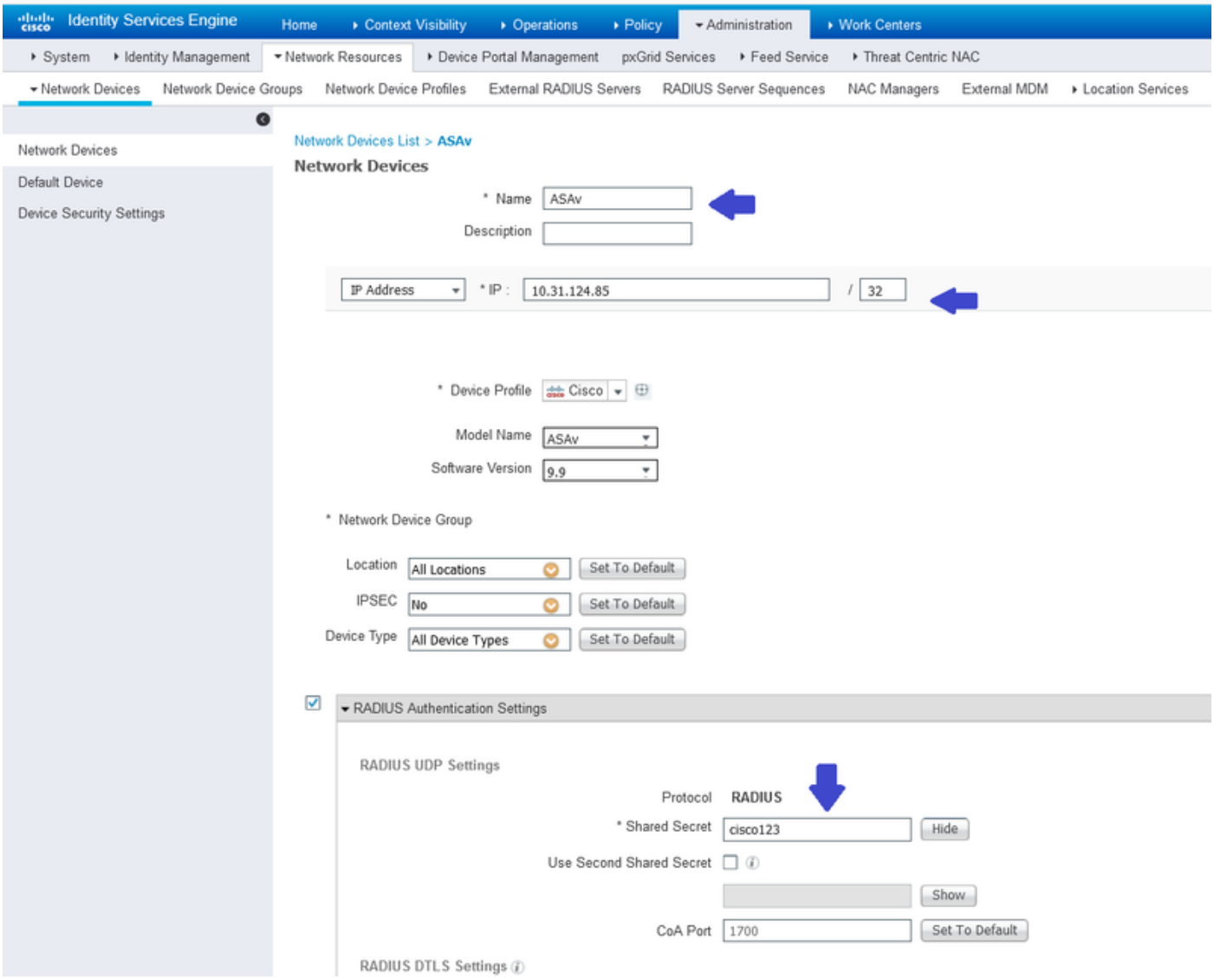
Nota: Con questo esempio di configurazione, è possibile assegnare i Criteri di gruppo a ciascun utente Anyconnect tramite la configurazione ISE. Poiché gli utenti non possono selezionare il gruppo di tunnel, sono connessi al gruppo di tunnel DefaultWEBVPNGroup e a

DfltGrpPolicy. Dopo l'autenticazione e la restituzione dell'attributo Class (Criteri di gruppo) nella risposta di autenticazione ISE, l'utente viene assegnato al gruppo corrispondente. Nel caso in cui all'utente non sia applicato un attributo Class, l'utente rimane comunque in DfltGrpPolicy. È possibile configurare gli **accessi simultanei vpn 0** nel gruppo DfltGroupPolicy in modo da evitare che gli utenti senza Criteri di gruppo si connettano tramite la VPN.

ISE

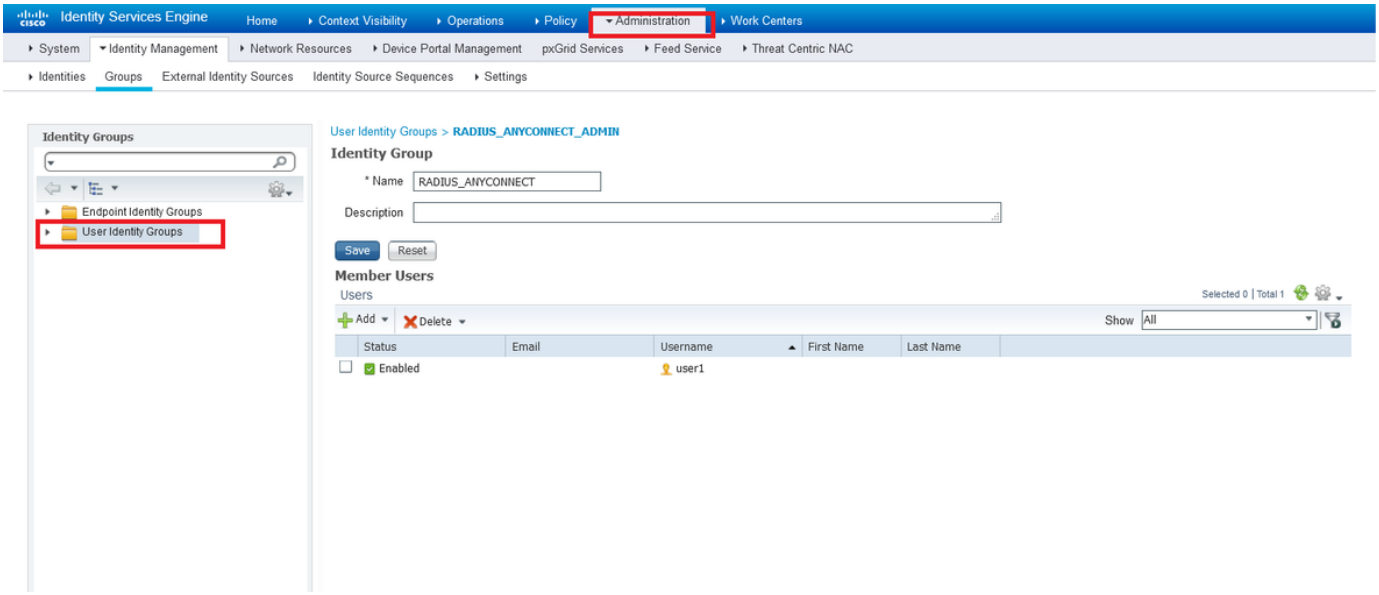
Passaggio 1. Aggiungere l'appliance ASA ad ISE.

Per questo passaggio, selezionare **Amministrazione>Risorse di rete>Dispositivi di rete.**



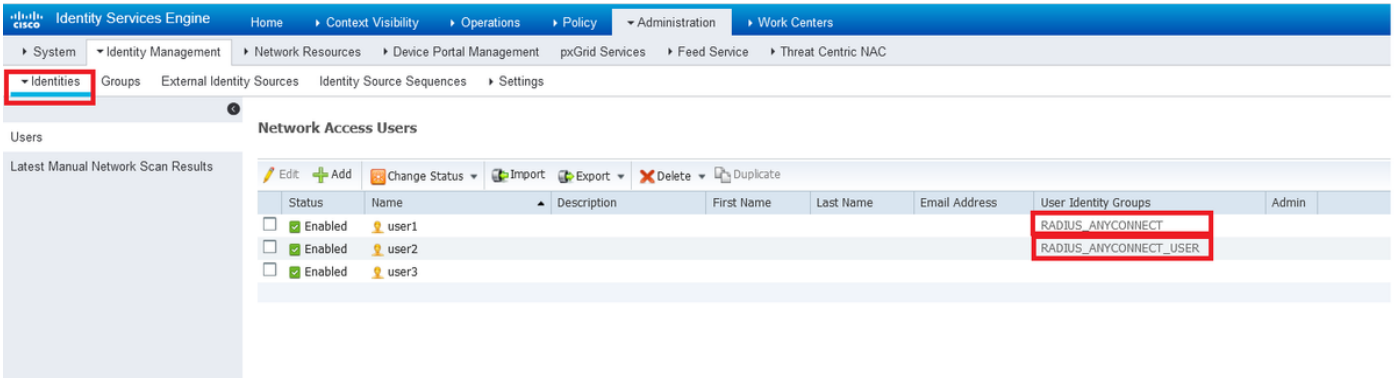
Passaggio 2. Creare gruppi di identità.

Definire i gruppi di identità per associare ciascun utente a quello di destra nei passi successivi. Passare a **Amministrazione>Gruppi>Gruppi identità utente.**



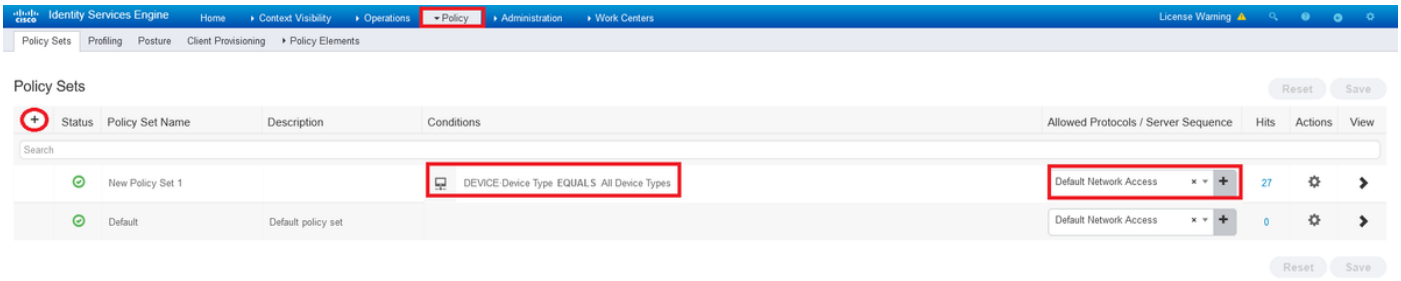
Passaggio 3. Associare gli utenti ai gruppi di identità.

Associare gli utenti al gruppo di identità corretto. Passare a **Amministrazione>Identità>Utenti.**



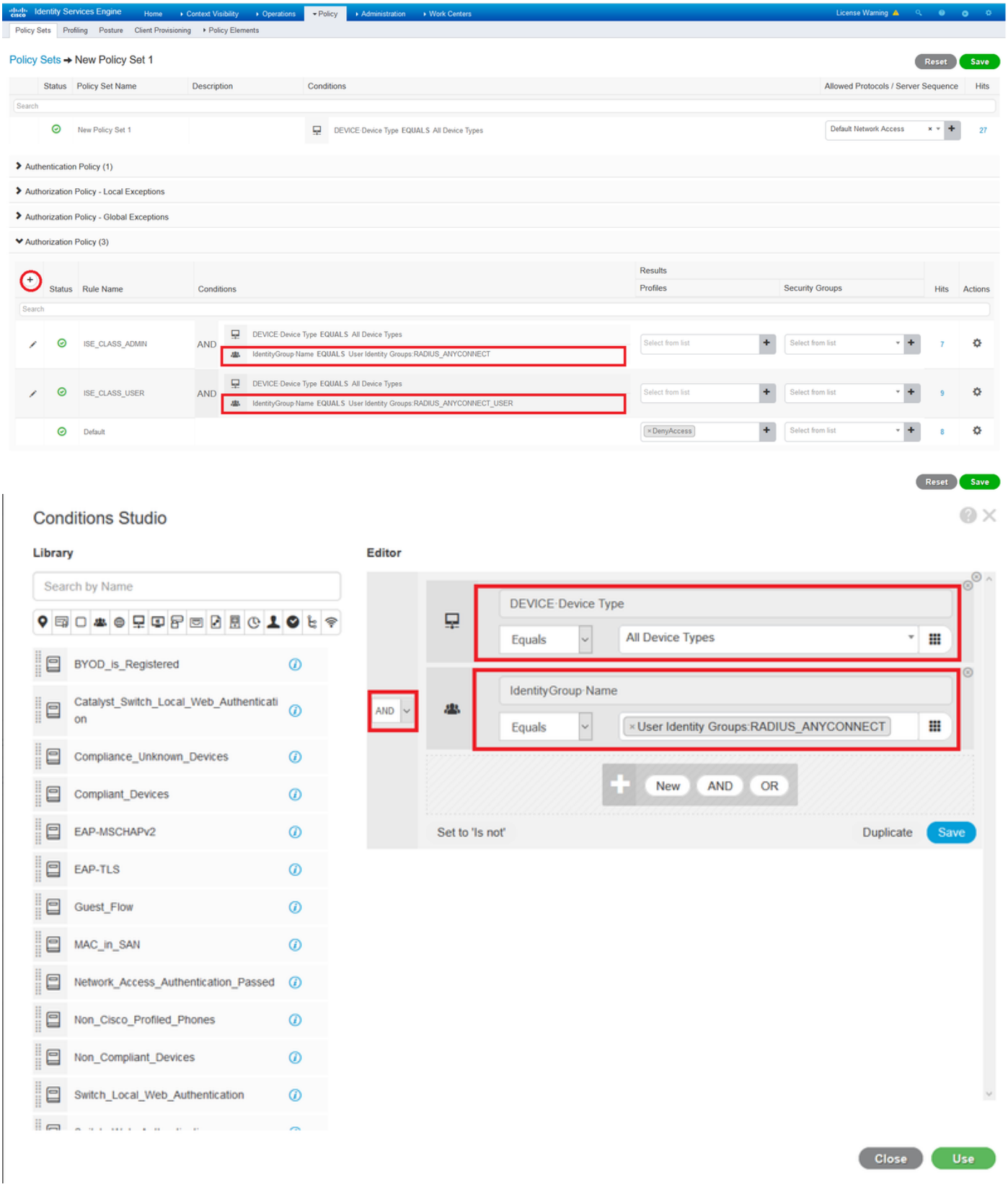
Passaggio 4. Creazione del set di criteri.

Definire un nuovo set di criteri come mostrato nell'esempio (tutti i tipi di dispositivi) in condizioni. Passare a **Criterio>Set di criteri.**



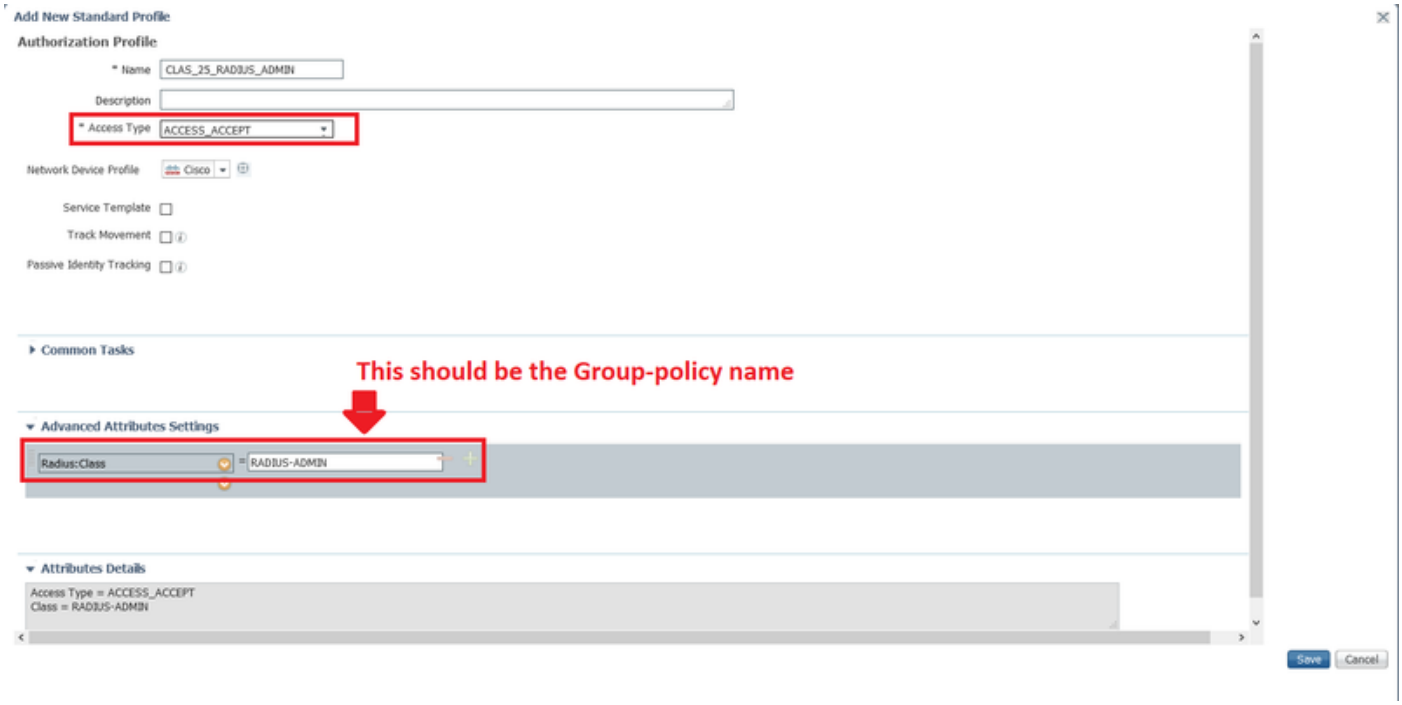
Passaggio 5. Creare un criterio di autorizzazione.

Creare un nuovo criterio di autorizzazione con le condizioni appropriate per corrispondere al gruppo di identità.

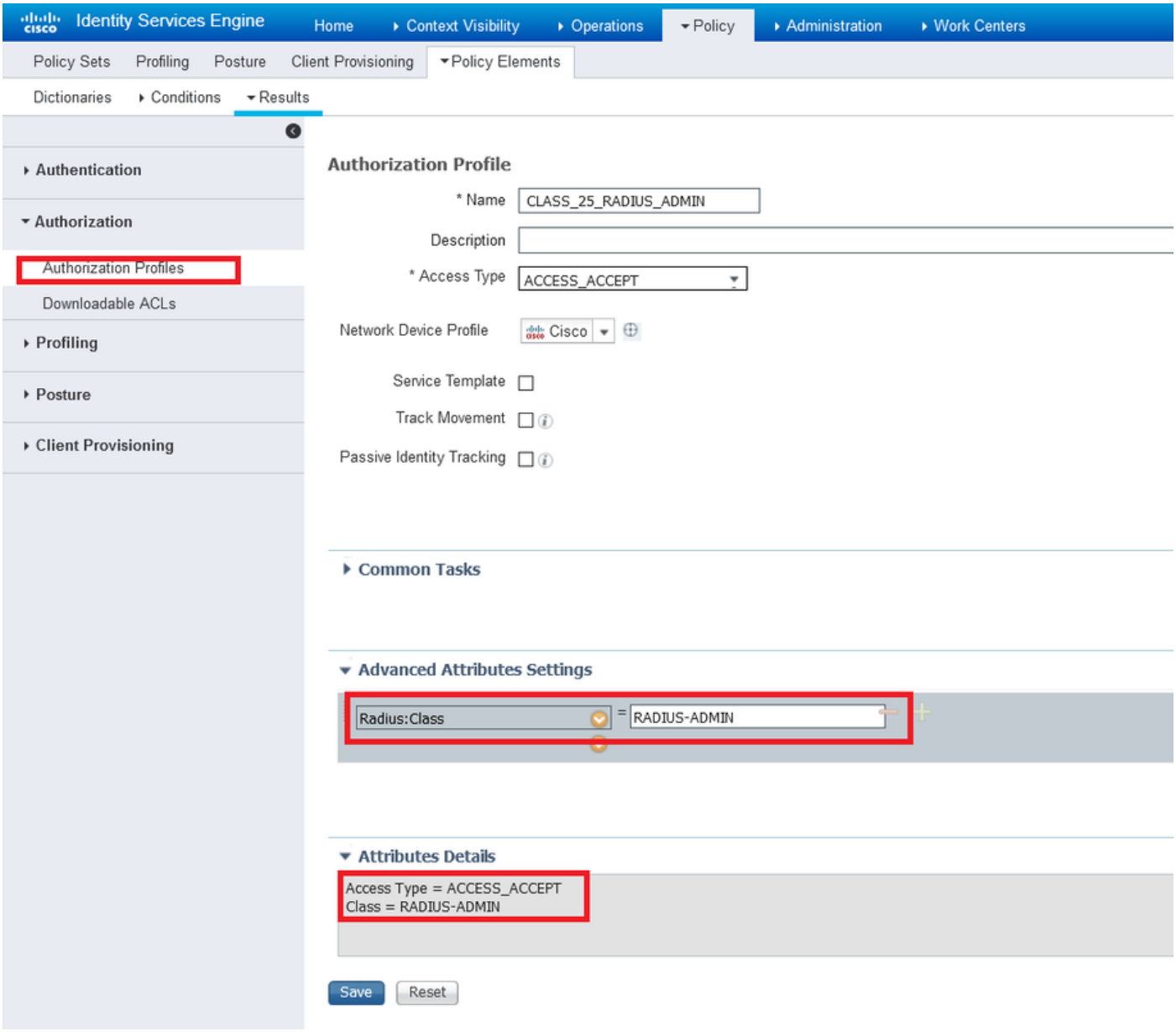


Passaggio 6. Creare un profilo di autorizzazione.

Creare un nuovo profilo di autorizzazione con RADIUS: Attributo Class<Group-Policy-ASA> e *Tipo di accesso: ACCESS_ACCEPT

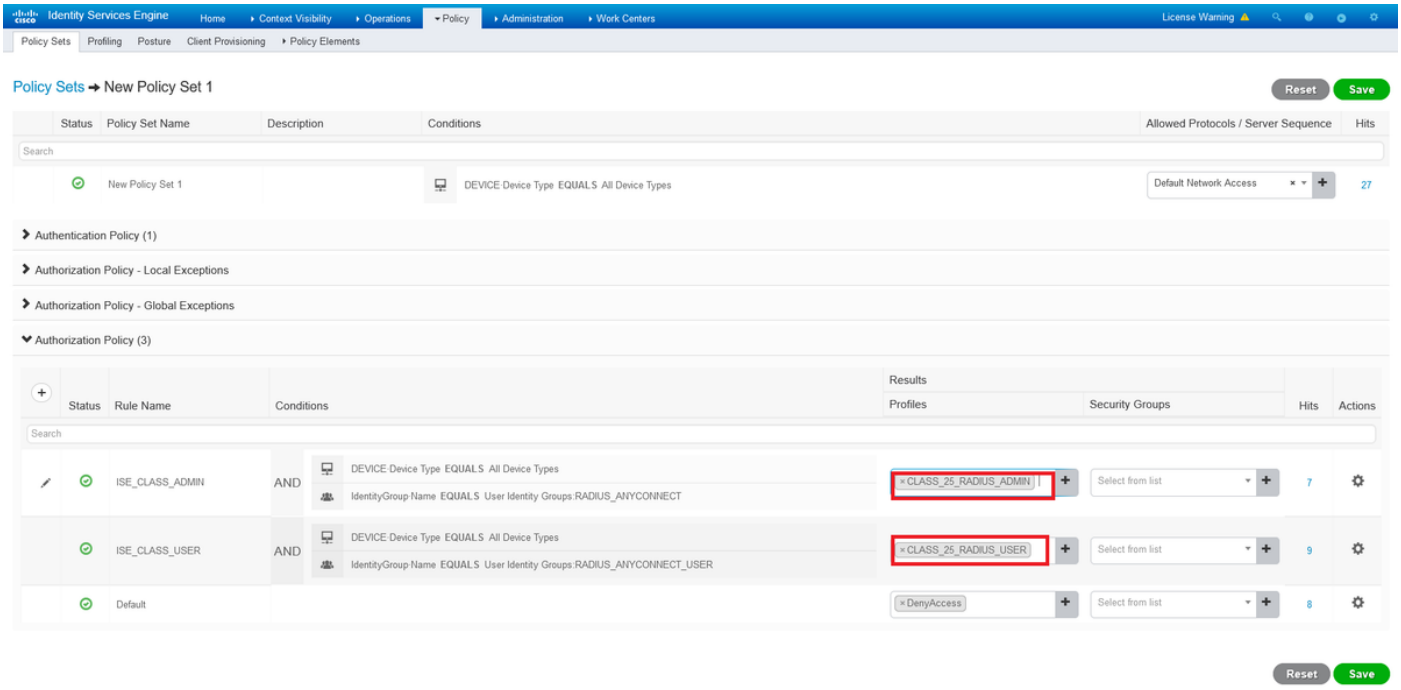


Passaggio 7. Verificare la configurazione del profilo di autorizzazione.



Nota: Seguire la configurazione come illustrato nell'immagine precedente, Access_Accept, Class—[25], RADIUS-ADMIN è il nome del criterio di gruppo (può essere modificato).

Nell'immagine è illustrato l'aspetto della configurazione. Nello stesso set di criteri non sono presenti criteri di autorizzazione, ognuno corrisponde al gruppo di identità necessario nella sezione ***condizioni*** e utilizza i criteri di gruppo disponibili sull'appliance ASA nella sezione ***profilo.***



Con questo esempio di configurazione, è possibile assegnare i Criteri di gruppo a ciascun utente Anyconnect tramite la configurazione ISE basata sull'attributo class.

Risoluzione dei problemi

Uno dei debug più utili è il **raggio di debug.** Mostra i dettagli della richiesta di autenticazione radius e della risposta di autenticazione tra il processo AAA e ASA.

```
debug radius
```

Un altro strumento utile è il comando test aaa-server. A questo punto, è possibile verificare se l'autenticazione è ACCETTATA o RIFIUTATA e se gli attributi (attributo 'class' in questo esempio) sono stati scambiati durante il processo di autenticazione.

```
test aaa-server authentication
```

Scenario di lavoro

Nell'esempio di configurazione riportato sopra, **l'utente 1** appartiene al gruppo **RADIUS-ADMIN** in base alla configurazione ISE, è possibile verificare se si esegue il test aaa-server e il comando debug radius. Evidenziare le righe da verificare.

```
ASAv# debug radius
ASAv#test aaa-server authentication ISE_AAA host 10.31.124.82 username user1 password *****
INFO: Attempting Authentication test to IP address (10.31.124.82) (timeout: 12 seconds)

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 84).....
01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73    |  ...T..|.X"5^.|Hs
04 9f 8c 74 01 07 75 73 65 72 31 02 12 ad 19 1c    |  ...t..user1.....
40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f 04 06 0a    |  @.C...F.5.R.o...
1f 7c 55 05 06 00 00 00 06 3d 06 00 00 00 05 1a    |  .|U......=......
```

```
15 00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d    |  .......coa-push=
74 72 75 65                                        |  true

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 30 (0x1E)
Radius: Length = 84 (0x0054)
Radius: Vector: ACB67CE55822355E8E7C4873049F8C74
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |  user1
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
ad 19 1c 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f    |  ...@.C...F.5.R.o
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.31.124.85 (0x0A1F7C55)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x6
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65             |  coa-push=true
send pkt 10.31.124.82/1645
rip 0x00007f03b419fb08 state 7 id 30
rad_vrfy() : response message verified
rip 0x00007f03b419fb08
 : chall_state ''
 : state 0x7
 : reqauth:
     ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74
 : info 0x00007f03b419fc48
     session_id 0x80000007
     request_id 0x1e
     user 'user1'
     response '***'
     app 0
     reason 0
     skey 'cisco123'
     sip 10.31.124.82
     type 1
```

RADIUS packet decode (response)

```
--------------------------------------
Raw packet data (length = 188).....
02 1e 00 bc 9e 5f 7c db ad 63 87 d8 c1 bb 03 41    |  ....._|..c.....A
37 3d 7a 35 01 07 75 73 65 72 31 18 43 52 65 61    |  7=z5..user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 52 71 51 47 52 72 70 36 5a 35 66 4e 4a    |  c52RqQGRrp6Z5fNJ
65 4a 39 76 4c 54 6a 73 58 75 65 59 35 4a 70 75    |  eJ9vLTjsXueY5Jpu
70 44 45 61 35 36 34 66 52 4f 44 57 78 34 19 0e    |  pDEa564fRODWx4..
52 41 44 49 55 53 2d 41 44 4d 49 4e 19 50 43 41    |  RADIUS-ADMIN.PCA
```

```
43 53 3a 30 61 31 66 37 63 35 32 52 71 51 47 52    |  CS:0a1f7c52RqQGR
72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 6a 73    |  rp6Z5fNJeJ9vLTjs
58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66    |  XueY5JpupDEa564f
52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f    |  RODWx4:iseamy24/
33 37 39 35 35 36 37 34 35 2f 33 31                |  379556745/31

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 30 (0x1E)
Radius: Length = 188 (0x00BC)
Radius: Vector: 9E5F7CDBAD6387D8C1BB0341373D7A35
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |  user1
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35    |  1f7c52RqQGRrp6Z5
66 4e 4a 65 4a 39 76 4c 54 6a 73 58 75 65 59 35    |  fNJeJ9vLTjsXueY5
4a 70 75 70 44 45 61 35 36 34 66 52 4f 44 57 78    |  JpupDEa564fRODWx
34                                                 |  4
Radius: Type = 25 (0x19) Class
Radius: Length = 14 (0x0E)
Radius: Value (String) =
52 41 44 49 55 53 2d 41 44 4d 49 4e                |  RADIUS-ADMIN
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 52 71 51    |  CACS:0a1f7c52RqQ
47 52 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54    |  GRrp6Z5fNJeJ9vLT
6a 73 58 75 65 59 35 4a 70 75 70 44 45 61 35 36    |  jsXueY5JpupDEa56
34 66 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32    |  4fRODWx4:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 31          |  4/379556745/31
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000007 id 30
free_rip 0x00007f03b419fb08
radius: send queue empty
INFO: Authentication Successful
```

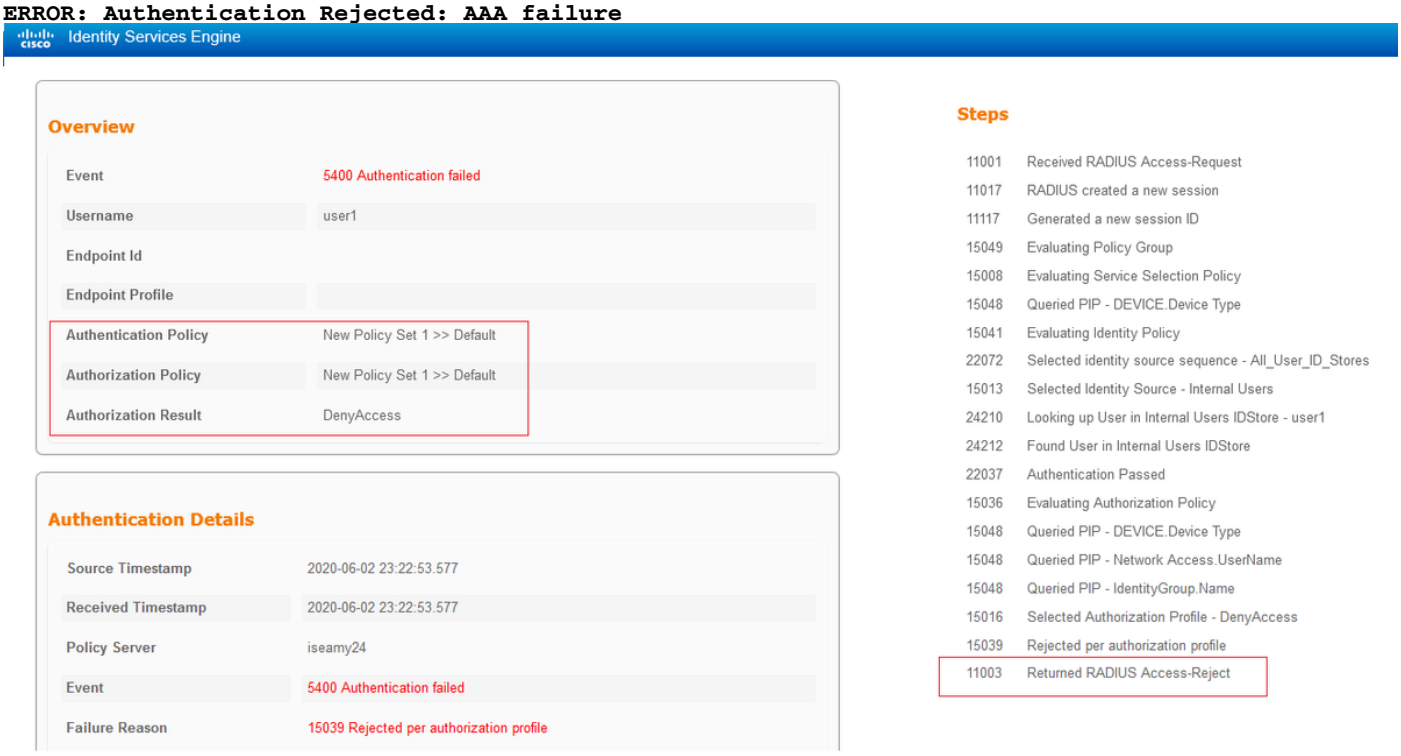
Per verificare se funziona quando l'utente 1 si connette tramite Anyconnect, usare il comando **show vpn-sessiondb anyconnect** per conoscere i Criteri di gruppo assegnati dall'attributo della classe ISE.

```
ASAv# show vpn-sessiondb anyconnect Session Type: AnyConnect  Username : user1                    Index
: 28
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15604                  Bytes Rx     : 28706
Group Policy : RADIUS-ADMIN           Tunnel Group : DefaultWEBVPNGroup
Login Time   : 04:14:45 UTC Wed Jun 3 2020
Duration     : 0h:01m:29s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001c0005ed723b5
Security Grp : none
```

Scenario non lavorativo 1

Se l'autenticazione non riesce su Anyconnect e l'ISE risponde con un REJECT. È necessario verificare se l'utente è associato a un **gruppo di identità utente** o se la password è errata. Passare a **Operazioni>Live Log > Dettagli.**

```
RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 20).....
03 21 00 14 dd 74 bb 43 8f 0a 40 fe d8 92 de 7a    |  .!...t.C..@....z
27 66 15 be                                        |  'f..

Parsed packet data.....
Radius: Code = 3 (0x03)
Radius: Identifier = 33 (0x21)
Radius: Length = 20 (0x0014)
Radius: Vector: DD74BB438F0A40FED892DE7A276615BE
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000009 id 33
free_rip 0x00007f03b419fb08
radius: send queue empty
ERROR: Authentication Rejected: AAA failure
```



Nota: In questo esempio, **user1** non è associato ad alcun **gruppo di identità utente.** Di conseguenza, viene eseguito il accesso ai criteri di autenticazione e autorizzazione predefiniti nel **nuovo set di criteri 1** con l'azione **DenyAccess**. È possibile modificare questa azione in **PermitAccess** nei criteri di autorizzazione predefiniti per consentire agli utenti che non dispongono del gruppo di identità utente di eseguire l'autenticazione.

Scenario non lavorativo 2

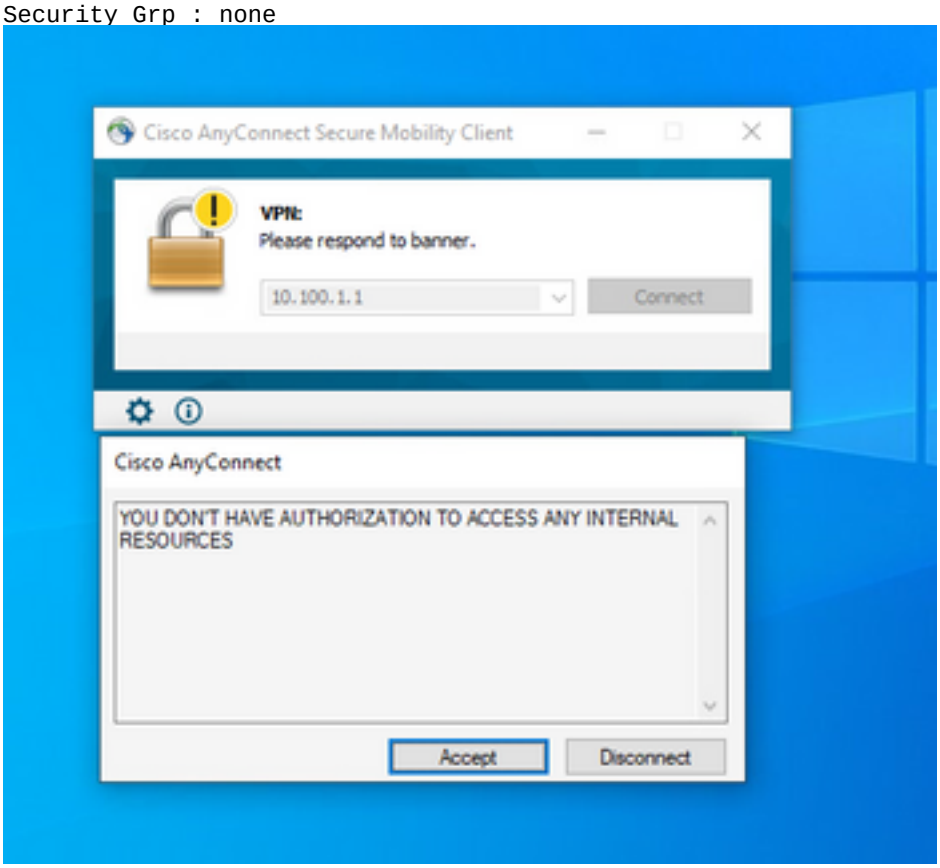
Se l'autenticazione non riesce su Anyconnect e il criterio di autorizzazione predefinito è PermitAccess, l'autenticazione viene accettata. Tuttavia, l'attributo class non è presentato nella risposta Radius, quindi l'utente si trova in DfltGrpPolicy e non si connetterà a causa di **vpn-simultous-login 0.**

```
RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 174).....
02 24 00 ae 5f 0f bc b1 65 53 64 71 1a a3 bd 88    |  .$.._...eSdq....
7c fe 44 eb 01 07 75 73 65 72 31 18 43 52 65 61    |  |.D...user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71    |  c5229Th3GhmDTI5q
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b    |  7HFE0zote4j7PviK
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50    |  Z5wqkxlP93BlJo.P
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 36 (0x24)
Radius: Length = 174 (0x00AE)
Radius: Vector: 5F0FBCB1655364711AA3BD887CFE44EB
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |  user1
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 32 39 54 68 33 47 68 6d 44 54    |  1f7c5229Th3GhmDT
49 35 71 37 48 46 45 30 7a 6f 74 65 34 6a 37 50    |  I5q7HFE0zote4j7P
76 69 4b 5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a    |  viKZ5wqkxlP93BlJ
6f                                                 |  o
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x8000000b id 36
free_rip 0x00007f03b419fb08
radius: send queue empty
INFO: Authentication Successful
ASAv#
```

Se l'opzione **vpn-simultous-logins 0** viene modificata in '1', l'utente si connette come mostrato nell'output:

```
ASAv# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : user1                    Index        :
```

```
41
Assigned IP  : 10.100.2.1            Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15448                 Bytes Rx     : 15528
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time   : 18:43:39 UTC Wed Jun 3 2020
Duration     : 0h:01m:40s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 0a640101000290005ed7ef5b
Security Grp : none
```



Scenario non lavorativo 3

Se l'autenticazione viene eseguita ma all'utente non vengono applicati i criteri corretti, ad esempio se al criterio di gruppo connesso è associato il tunnel suddiviso anziché il tunnel completo come deve essere. L'utente potrebbe trovarsi nel gruppo di identità utente errato.

```
ASAv# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                 Index        : 29
Assigned IP  : 10.100.2.1            Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 15592                 Bytes Rx     : 0
Group Policy : RADIUS-USERS          Tunnel Group : DefaultWEBVPNGroup
Login Time   : 04:36:50 UTC Wed Jun 3 2020
```

```
Duration     : 0h:00m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001d0005ed728e2
Security Grp : none
```

Video

In questo video viene illustrato come configurare Anyconnect SSL con autenticazione ISE e attributo di classe per Group-Policy Mapping.